Chinese guided missile destroyer *Shenzhen* departing Apra Harbor, Guam, 2003

U.S. Navy (Nathanael T. Miller)

Chinese and American Network Warfare

By TIMOTHY L. THOMAS

China published a fourth version of its white paper on national defense in December 2002.[1] The document received positive comments from U.S. analysts for its greater sophistication than previous versions and mild criticism for its continued lack of detail. Subjects addressed included China's security situation, defense policy, armed forces, international security cooperation, and arms control and disarmament. But there was a noticeable lack of attention to *information warfare* (IW) and *information operations* (IO), subjects to which the congressionally mandated DOD study, "The Military Power of the People's Republic of China," paid particular attention in 2002.[2] In addition, China's 2004 white paper failed to address IW but focused on the revolution in military affairs and the topic of informationalization, which was mentioned more than 20 times.

This 2002 white paper, however, did note that information technologies (IT) have helped stretch the battlefield into "multidimensional space, which includes the land, sea, air, outer space, and electron." The last term, in U.S. documents, usually refers to the information sphere. The form of war, the paper added, is becoming information oriented. High technology was listed as an acquisition priority, and 20,000 kilometers of fiber optic cable was laid in western China, while in October 2000 the General Staff organized a computer networking and electronic countermeasure exercise

Timothy L. Thomas is assigned to the Foreign Military Studies Office at Fort Leavenworth, Kansas.

around Beijing. Finally, the paper noted that in 2001, many People's Liberation Army (PLA) studies and exercises explored the features and patterns of an integrated network-electronic warfare (INEW) concept. Thus, while not specifically highlighting IW or IO, information-related topics were mentioned.

INEW is worthy of further note. Earlier in 2002, in the journal *China Military Science*, Major General Dai Qingmin, head of the 4th Department of the General Staff, explained the concept, which he had first mentioned in the August 2000 issue of that journal. Parts of Dai's 2002 article contradicted the white paper. For example, he stated that the concept placed more emphasis on active offense, whereas the paper emphasized a traditional active defense focus. Dai equated INEW with IO, which the white paper did not, noting that it "serves as information operations theory with Chinese characteristics." It is strange that the 2002 Pentagon report on China did not mention this concept, a theory that appears to be a half cousin to the wildly popular Pentagon transformation concept of *network-centric warfare* (NCW).

many People's Liberation Army studies and exercises explored an integrated network-electronic warfare concept

This article compares General Dai's INEW concept with the U.S. network-centric warfare concept and highlights their strengths and weaknesses. Many issues arise. For example, both concepts evade the fog and friction of war, assuming perfect information and ignoring those problems at their own peril. Further, both are bathed in their own cultural environments. The United States used a business metaphor when discussing NCW. Dai, on the other hand, noted that INEW refers to an overall concept, method, and strategy for guiding IO, not a set of hardware and software or a single system, and puts "the wings of network warfare on traditional electronic warfare." Clearly, moving from kinetic to network-based warfare will be an interesting transformation as different nations look at new developments in their own ways.

Integrated Network-Electronic Warfare

Dai's 2002 article, "On Integrating Network Warfare and Electronic Warfare," noted several topics of interest:

- IO contradictions
- IO centers of gravity
- network weaknesses
- importance of IT training
- achieving information superiority
- definitions of information war and other terms, all with Chinese characteristics.[3]

Dai argues that information warfare is composed of six "forms": operational security, military deception, psychological war, electronic war (EW), computer network war, and physical destruction. He made only one further reference to psychological operations in the article and never again mentioned operational security, military deception, and physical destruction. Electronic warfare and computer network warfare thus captured most of his attention.

INEW, according to Dai, refers to a series of combat operations that use the integration of electronic warfare and computer network warfare measures to disrupt the normal operation of enemy battlefield information systems while protecting one's own, with the objective of seizing information superiority—similar to the U.S. definition of IO. While network war disrupts processing and use of information, EW disrupts acquisition and forwarding of information. The core of computer network warfare is to "disrupt the layers in which information is processed, with the objective of seizing and maintaining control of network space." EW is targeted at networked information systems and informationalized weapons in order to increase combat effectiveness. INEW is essential for the system-versus-system confrontation on the informationalized battlefield.

Dai did not use the term *network centric*, although there seem to be similarities between his and American concepts. For example, a subtitle on the cover of a U.S. publication, *Network Centric Warfare*, states that the concept is for "developing and leveraging information superiority." The INEW objective, according to Dai, is not to develop and leverage but simply to seize information superiority.

INEW emphasizes integrating combat operations by merging command, forces, objectives, and actions. Command integration is its unified planning, organization, coordination, and control. Forces integration is its use in a complementary manner. Objective integration is its simultaneous use against enemy command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^{4}ISR), while action integration is its coordination to produce combined power. Dai listed the characteristics of INEW as its comprehensive nature, its integrated methods and expansive nature ("battlespace"), and the integrated nature of its "effectiveness."

Launching AsiaSat–6 communication satellite aboard Chinese-made Long March 3B rocket from Xichang, April 12, 2005

AP/Wide World Photo (Li Gang Xinhua)

Forces integration implies the synthesis of platforms with networks.

The concept has a comprehensive effect on the enemy when it destroys C^{4}ISR, according to Dai, thereby constraining decisionmaking and strategic planning. C^{4}ISR systems are integrators and force multipliers, the focal point of IO. Dai did not address what would happen if INEW only damaged or disrupted systems, but one can imagine that the effects would be severe if not disabling. Integrated INEW methods can be developed into a unified plan and organization for action, and the expansive nature of battlespace (Dai implies an informationalized battlefield replete with information-based systems) allows for noncontact and nonlinear operations as well as full-depth integrated attacks. Finally, the main targets are enemy military, political, economic, and social information systems, making the potential effectiveness greater than any traditional combat operation form.

information operations revolve around destroying enemy systems and protecting friendly ones

Information operations revolve around destroying enemy systems and protecting friendly ones. Acquiring and forwarding information relies on electronic warfare, while processing and using the information relies on computer networks. INEW provides the means to participate in the system-versus-system confrontation and for attaining information superiority since systems are centers of gravity for combat forces. People and weapons become insignificant when not structured within a system. This concept appears similar to the U.S. idea of systems integration except for its emphasis on ideology and philosophy. However, nowhere does Dai entertain fog and friction in the information age; he presents his argument as if there were no such problems.

The Chinese see the main combat contradiction as being between starting and stopping the flow of information in both the electromagnetic sphere and the space occupied by networks. An example of a successful operation would be disrupting information processing and obtaining control over network space, thereby disrupting the enemy knowledge system and preventing commanders from obtaining information required to make decisions. The struggle for information superiority is vital since it is a precondition for seizing sea, air, and space superiority.

When discussing China's "two transformations," Dai again emphasized the active offense. He noted that the first transformation means changing from just EW to several forms and methods, such as INEW. The second transformation is to emphasize both defense and offense, with the "priority being the development of offensive information operations equipment." Again, this goal directly contradicts the emphasis in the white paper on the active defense. It is not clear whether the Chinese deliberately downplayed offensive operations in the information age or it was a rebuff to Dai's article. With regard to strategy, Dai noted that China must make breakthroughs at weak points, seize the commanding high ground, leap out of dead ends, coordinate development, and grasp key junctures.

Finally, Dai noted that implementing INEW required an "information warfare personnel development plan." Information operations command personnel who understand technology and can manage as well as staff personnel and trainers are needed to teach and carry out ideological work. Combat personnel are needed to study, research, train, and fight. Finally, it is necessary to develop competencies for merging networks and electronics. Academies must develop specialized courses, deepen reforms, and send large numbers of multitalented IO personnel to units.

Putting the INEW plan into action will require the use of theoretical achievements and modeling the battlefield deployment and other situational aspects of an enemy force. Perhaps this is being accomplished via computer network brigades or reserve IW units serving as opposition forces against the PLA. In China, theory guides training, and rules and regulations are produced from evaluating the training.

Most likely, Dai's article was condensed from his earlier work. One critique of that work stated that the concept of INEW demonstrated that China no longer only learns from foreign militaries but has developed innovative theories with special Chinese military features. Further, the critique reiterated (as did Dai's 2002 article) that systems represent the center of gravity of combat forces and that systems integration uses information as a control mechanism to form a combat capability greater than the sum of its parts. To American IO theorists, however, the Chinese approach does not appear to have as many special "Chinese characteristics" as it purports. INEW sounds similar to American theory of a few years ago, when system-of-systems research was more fashionable.

traditional strategic theories are being rethought, new strategies mapped out, and new confrontation strategies advanced

In fact, not only Chinese but also some U.S. commanders highly regard electronic warfare, even at the expense of computer network attack. For example, General Hal Hornburg, USAF, Chief of Air Combat Command, noted that IO should be separated into three areas: manipulation of public perception, computer network attack, and electronic warfare. Only the latter should be assigned to the warfighter.[4]

In the 2000 article Dai stated that the means of integrated application of information fighting will initially be the integrated application of networks and electronics and that the key to gaining the initiative in IO lies in the establishment of an "active offensive." Dai also noted that an IO is a series of operations with an information environment as the basic battlefield condition, with military information and an information system as the direct operational targets, and with EW and a computer network war as the principal forms.[5]

Dai further noted that information operations are both confrontations focusing on forces and arms and, more importantly, trials of strength focusing on knowledge and strategies, meaning the emphasis should be on strategies. As technology has reinforced human initiative, it has also highlighted the role played by a confrontation of strategies. Now traditional strategic theories are being rethought, new strategies mapped out, and new confrontation strategies advanced.

Network-Centric Warfare

In 1998, Vice Admiral Arthur Cebrowski, USN (Ret.), the director for space, information warfare, and command and control (N–6), and John Garstka, the scientific and technical advisor for the directorate for C[4] systems on the Joint Staff (J–6), wrote an article focused on business adaptations to the information age:[6]

- The power of network-centric computing comes from information-intensive interactions between large numbers of heterogeneous computational nodes in the network.
- Competitive advantages come from the co-evolvement of organizations and processes to exploit information technology, employing network-centric operational architectures consisting of a high-powered information grid, a sensor grid, and a transaction grid.
- The key to market dominance lies in making strategic choices appropriate to changing ecosystems.

The authors then noted that network-centric operations offered the same dynamics to the military. Strategically, that meant understanding all the elements of battlespace and battle time; operationally, it meant mirroring business ecosystem linkages among units and the operating environment; tactically, it meant speed of operations; and structurally, it meant that network-centric warfare required sensor and transaction grids and an information grid supported by command and control processes needing automation for speed. Network-centric warfare reportedly enabled a shift from attrition warfare. Speed enabled a force to have more battlespace awareness, mass effects instead of forces, and foreclose enemy courses of action. It also offset disadvantages in numbers, technology, or position and was capable of locking out alternative enemy strategies and locking in success.

This list is significantly different from Dai's, with its focus on contradictions, ideology, and centers of gravity. This is not surprising since different cultures will interpret the interaction of systems in different ways. Of concern, however, is once again the notable absence of focus and discussion on the fog and friction of technology in a real-time battlespace. The U.S. concept appears to rely on speed to overcome all obstacles. The concept seems to focus on "the content, quality, and timeliness of information moving between nodes on the network" and dismisses misinformation or deception. Loren Thompson, chief operating officer of the Lexington Institute, commented about overreliance on business strategies while critiquing a 2002 article by Admiral Cebrowski on NCW:

> *Let me conclude by answering Cebrowski's question as to why commercial development cycles are so much shorter than military ones. The reason is that it's harder to get to geocentric orbit than the grocery store, that no one is shooting at the Coca Cola Company, and that private-sector executives don't rewrite their business plans every time a consultant comes up with a new idea.*[7]

There also appear to be built-in contradictions in the concept. For example, the authors note that NCW strength is designed to "offset a disadvantage in numbers, technology, or position." Further, "We must change how we train, organize, and allocate resources if the United States decides to fight on an NCW rather than a platform-centric basis."[8] Yet the authors twice note that a sensor or engagement grid must be coupled in time to shooters, and the DOD report to Congress on NCW stated, "Battlefield entities (platforms, units, sensors, shooters) must be designed 'net ready.'"[9] This reliance on interoperability is not given the place it deserves by U.S. theorists. This interoperability resembles the integration process the Chinese stress.

reliance on interoperability is not given the place it deserves by U.S. theorists

Cebrowski and Garstka underscored that NCW made the whole greater than the sum of its parts, which the Chinese INEW concept also noted, with the latter perhaps mimicking the American authors. In contrast to the Chinese, Cebrowski and Garstka used the term *system* sparingly; however, systems remain important to the U.S. concept.

David Alberts, John Garstka, and Frederick Stein wrote *Network Centric Warfare* in 1999. The book defines *NCW* as: an information superiority–enabled concept of operations that generates increased combat power by networking sensors, decisionmakers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization.[10] The authors imply integration of platforms and networks by including sensors and shooters in their definition. Again, however, fog and friction are ignored.

In October 2002, Cebrowski wrote that any weapons system must be on the net to remain viable—the concept of a net-ready platform. If such interoperability is not available, the program is subject to cancellation. Risk is managed by increasing the breadth of capabilities to cover gaps.[11] Can simply increasing capabilities reduce fog and friction? Don't surprise or disruption mean anything for theory? Cebrowski also noted that aircraft and other joint capabilities in Afghanistan were empowered by high-speed NCW principles. However, problems remained, such as minimal information filtering and decision aids for field commanders.

The DOD report to Congress about NCW stressed many of these points.[12] It noted that interoperability must not be abandoned ("a critical mass of connectivity and interoperability is necessary to both encourage and support new ways of doing business") and that impediments to the program must be overcome. However, the report does assert that "NCW is to warfare what e-business is to business" and "no single platform or sensor is the heart of the system." The first statement again overemphasizes the business-military comparison, and the latter implies that platforms remain vital to the NCW concept. We are not moving from platform to NCW, but from platform to an integrated or interoperable form of platforms and nets.

Chinese IW expert Wang Baocun, writing in *China Military Science*, discussed the U.S. concept of network-centric warfare from a Chinese perspective. He did not compare NCW with INEW, although he noted that China must study the theoretical and practical aspects of other countries' efforts to develop an information-based military in order for China to do the same. He further stated that China must develop a comprehensive electronic information system and that such systems should be integrated.[13] To that degree, Wang appears to echo Dai.

Comparing NCW and INEW

The two explanations above represent the basic views of Chinese and U.S. specialists on network-related concepts. Clearly these are ideas for the present and immediate future and will form the basis of both countries' transformations. However, the terms should be examined against other paradigms as well. Admiral Cebrowski is a proponent of alternate or even multiple concepts. He stressed that "one best way" should not be pursued, as there may not be one architecture or standard. Rather, competing concepts should be debated. And interestingly enough, the view from a "bottom-up" perspective is different from the view at the top. Those at the bottom have other points for the authors to consider.

First, it is unfortunate that the authors who proposed these concepts did not venture into detailed definitions, for this lack has confused readers. For example, Cebrowski and Garstka used the terms *network-centric computing*, *network-centric operations*, and *network-centric war* in their seminal article without defining them. Readers were left with the impression that they are interchangeable sound bites for an idea. A citation at the end regarding NCW came closest to a definition, noting that it is "applicable to all levels of warfare and contributes to the coalescence of strategy, operations, and tactics. NCW is transparent to mission, force size and composition, and geography." This description was updated in *Network Centric Warfare*, by Alberts, Garstka, and Stein, which Cebrowski reviewed. Their definition is better but still needs specification, such as an explanation of what a network "war" means. Would *confrontation* or *struggle* work better, for example? Do networks really war with one another?

The terminology problem is important because if we are attempting to sell a concept, we need a thorough understanding of what we are selling. The authors appeared to be describing warfare enabled by speed of awareness and shared knowledge to bring effects to bear on targets in a timely and accurate manner. Thus, NCW is an enabler much like other developments in the mechanized age, albeit a quantum leap, to act as a combat facilitator, especially of battlefield awareness. Communications have always acted as enablers, facilitators, and coordinators of battlespace awareness, just not to the same degree as sensors and satellites. Terms such as *network-assisted platform operations*, *network-coordinating engagement operations*, or simply *network-centric operations* appear as appropriate as network-centric warfare. The INEW concept suffers from the same imprecision. In many ways it sounds like an updated version of NCW except for its EW and stratagem links.

AP/Wide World Photo (Greg Baker)

China Netcom technicians connect lines in Beijing

Second, many NCW authors describe a movement away from platforms to networks in their discussion of theory, then use an integrated or interoperable model of platforms and networks to describe their concept, which again shows lack of precision. Further discussion of the move from kinetic to combined kinetic, electronic, and network-based warfare would have assisted understanding. NCW does not occur in isolation. If it did, no one could use it because it would not control or be connected to anything; it would just be a grouping of sensors and nodes joined to a network that produces information. Rather, the concept implies that sensors are part of systems integrated into platforms. Weapons, weapons systems, and platforms are plugged into the sensor, information, and transaction grids that comprise NCW at the moment, and they will be with us for some time. Platforms launch weapons and have nodes where network information is integrated into the targeting and protection mechanisms of the platform. Predators are platforms that use networks.

AP/Wide World Photo (Li Gang Xinhua)

Space Control Center in Beijing monitoring return of China's first astronaut, October 16, 2003

The INEW concept used the word *integrated* while NCW theorists used *interoperable* for KC–135 aerial refuelers that possess routers, antennas, and other equipment so the aircraft can transmit battlespace information among units.

Third, the NWC discussion suggests that the concept alone is sufficient to make a nation great and modern. The American metaphor is that if it works for business, it will work for the military. The difference is that in the military, people plan on destroying the networks through high-tech weapons, making the systems useless. Or they try to deceive sensors and satellites, which does not happen often in business because it runs on information in a more perfect form. The military does not possess perfect information to the degree the market does; therefore, economic superiority may not translate into military superiority. Most important, there is no discussion of what might happen if such a system meets a like system or if there is even partial disruption. Kosovo, Somalia, and Bosnia were not confrontations between modern systems, but rather of modern against antiquated systems. So there is little consideration of the impact of the fog and friction of war on NCW and INEW. And there remain problems of available bandwidth, mission priorities and access to networked platforms, and the number of combat systems that must be coordinated—over 400 by some accounts.

the American metaphor is that if it works for business, it will work for the military

Fourth, the network-centric concept is technology-focused, while INEW possesses a strong stratagem element. This difference is important. It is how INEW plans to "defeat the superior with the inferior." The Chinese have noted that Asian analysts think in terms of stratagems and Western planners in terms of technology. Western strategists should be aware of this perspective.

Alfred Kaufman, a study director at the U.S. Institute for Defense Analyses, agrees that technology has too prominent a place in our military thinking, so much so that it dictates military strategy. He wrote that NCW theory has resulted in "the virtual collapse of the intellectual structure that was erected to control the development of Western military technology." He believes that the Pentagon hopes that commercial innovation will bring to war and to national security the same benefits it brings to commercial enterprises. In his view, NCW is flawed because it:

- overestimates man's capacity to deal with contradictory information
- ignores the true nature of the enemy and drives him to asymmetric strategies
- ignores the dynamic nature of combat and bureaucratizes war
- assumes that military victory is an end in itself.[14]

Fifth, consideration is given to the human in the loop, yet one wonders if a proper parallel should be drawn between NCW/INEW and human network attacks (HNA). NCW and INEW discuss the importance of training and educating personnel to conduct themselves as well as to run a network-oriented staff. U.S. theory now includes discussions of effects-based operations to demonstrate how NCW can be used to affect humans and objectives in a sequenced manner. Addressing the human as a network might be the next logical thinking. HNA refers to the ability of weapons, including nonlethals, to shut down the operating systems of people, who have their electric circuitry in the form of neurons. Properly targeted, this type of attack can make it difficult for humans to enter the decisionmaking cycle to assist in processing and selecting targets, the failsafe aspect to NCW and INEW.

Sixth, the United States needs to study foreign IO and NCW related concepts if it is to understand how to work with or against the cyber age systems of other countries. It is clear that China studies Pentagon thinking. At Chinese book stores there are hundreds of U.S. books translated from English, especially in the IO area. No such bounty on Chinese thinking can be found in American book stores.

Finally and most importantly, Dai noted that INEW is an offensive strategy based on acquiring both defensive and offensive information operations equipment, "with the priority being the development of offensive information operations equipment." Further, it is "important to take the initiative and effectively destroy the enemy's electronic information systems."[15] The focus on the active offense is lacking in NCW discussions, as is the Chinese focus on applying strategies to offset inferiorities in technology and equipment. The latter focus is really on the decisionmaker's mind, with strategies being the means and perception management the ends.

The good news is that the initial discussion of NCW is over, and the concept has received feedback from both private and public sources. This has provided substance to Admiral Cebrowski's foresight that more than one idea should be pursued. China is lacking in that area. The INEW topic has not been publicly critiqued. Perhaps the dialectic of point and counterpoint works better in Western culture based on its willingness to confront ideas with counters or better ideas. In many ways, China merely mirrors what happens in the West in the network-centric arena, but the West must be acutely aware of the Chinese nuances and mirror imaging.

U.S. decisionmakers, many with business backgrounds, must not apply their business experience to the military arena. The concept worked well, but in an environment totally divorced from the battlefield. China, on the other hand, will continue to load its INEW concept with Chinese characteristics, or so they say. Their metaphor will be shaped by the words of famous strategists and consider the use of deception and surprise while the United States focuses on speed of response and efficiency. One important distinction in the Chinese approach, however, is that INEW would be used to attack economic, political, societal, and military networks.

Does U.S. strategy risk overdependence on speed and prowess at the expense of other factors, while China tries to defeat the superior with the inferior, using good but not outstanding technology combined with stratagems? Both concepts lack ways to block failure in an age of continued fog and friction. We are uncertain what happens if our risk-taking fails. No one wants to talk about that. And, as the conflict in Iraq extends and diverts funding from the transformation effort, we may be closer than we think to confronting the risks discussed here. **JFQ**

NOTES

[1] *China's National Defense in 2002*, white paper (Beijing: Information Office of the State Council of the People's Republic of China, December 2002), available at <www.aseansec.org/ARF/ARF-DWP/China-2002.doc>.

[2] See *Annual Report on the Military Power of the People's Republic of China* (Washington, DC: Department of Defense, July 2002).

[3] Dai Qingmin, "On Integrating Network Warfare and Electronic Warfare," *Zhongguo Junshi Kexue* (*China Military Science*) (February 2002), 112–117, as translated and downloaded by the Foreign Broadcast Information Service (FBIS) Web site.

[4] David Fulghum, "USAF Redefining Boundaries of Computer Attack," *Aviation Week and Space Technology* 158, no. 9 (March 3, 2003), 33.

[5] "Introduction to Integrated Network-Electronic Warfare," *Jiefangjun Bao* (February 26, 2002), 6, accessed at <https://www.fbis.gov/>.

[6] Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *U.S. Naval Institute Proceedings* 124, no. 1 (January 1998), 28–35.

[7] Loren Thompson, "Dot-Com Mania," *Defense News*, October 28–November 3, 2002, 12.

[8] Cebrowski and Garstka.

[9] Art Money, *Report on Network Centric Warfare: Sense of the Report*, March 2001, accessed at <http://www.dodccrp.org/NCW/NCW_report/report/ncww_cover.html>.

[10] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare* (Washington, DC: National Defense University Press, 1999), 2.

[11] Arthur K. Cebrowski, "New Rules, New Era: Pentagon Must Embrace Information Age," *Defense News*, October 21–27, 2002, 28.

[12] *Annual Report*.

[13] Wang Baocun, "The Future Warfare for Which the U.S. Military Is Making Preparations: Network-Centric Warfare," *Zhongguo Junshi Kexue* (*China Military Science*) (October 2002), 133–143, as translated and downloaded by FBIS.

[14] Alfred Kaufman, "Caught in the Network," *Armed Forces Journal* (February 2005), 20–22.

[15] Dai Qingmin.